KING & SPALDING, LLP

1180 Peachtree Street NE
Atlanta, Georgia 30309-3521
Telephone: 404/572-4600
Facsimile: 404/572-5100
www.kslaw.com

FAX TRANSMITTAL SHEET

December 8, 2006

TO:	**Mail Stop Appeal Brief-Patents** Commissioner for Patents U.S. Patent Application No. 10/066,367	**Company:**	U.S. Patent and Trademark Office
	Fax #: 571-273-8300	**City/State:**	Alexandria, VA 22313
FROM:	Kerry L. Broome 3443	**Our Ref. #:**	05456.105009

NUMBER OF PAGES (including transmittal sheet): 28

If transmission problems occur or you are not the intended recipient, please call 404.572.2459 immediately. Thank you.

Notes/Comments:

Documents Submitted Via Facsimile:

Applicant:	Robert David Zobel et al.
Serial No.:	10/066,367
Filed:	January 31, 2002
For:	Method and System for Configuring and Scheduling Audits of a Computer Network
Papers Faxed:	Transmittal for Appeal Brief in duplicate (2-pgs.); Appeal Brief (25-pgs.).

RECEIVED
CENTRAL FAX CENTER

DEC 08 2006

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: **Robert David Zobel et al.**	Atty Docket: **05456.105009**
Application No.: **10/066,367**	Art Unit: **2135**
Filing Date: **January 31, 2002**	Examiner: **Yin Chen Shaw**
Title: **Method and System for Configuring and Scheduling Audits of a Computer Network**	Confirmation No.: **2476**

TRANSMITTAL FOR APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants hereby appeal to the Board of Patent Appeals and Interferences from the last decision of the Examiner dated October 18, 2006.

Please charge Deposit Account No. 11-0980 in the amount of $500.00 for the fee for filing a brief in support of the appeal required under 37 C.F.R. § 41.20(b)(2).

The Commissioner is authorized to charge any additional fee required for this Notice of Appeal, or to credit any overpayment, to Deposit Account No. 11-0980. A duplicate of this paper is enclosed.

Respectfully submitted,

Kerry L. Broome

KING & SPALDING LLP
1180 Peachtree Street, N.E., 34th Floor
Atlanta, Georgia 30309-3521
(404) 572-4600

Kerry L. Broome
Attorney for Applicants
Reg. No. 54,004

I hereby certify that this correspondence is being facsimile transmitted to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450, Facsimile No. (571) 273-8300, on December 8, 2006.

Kerry L Broome

Kerry L. Broome, Reg. No. 54,004

Patents

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: **Robert David Zobel et al.**	Atty Docket: **05456.105009**
Application No.: **10/066,367**	Art Unit: **2135**
Filing Date: **January 31, 2002**	Examiner: **Yin Chen Shaw**
Title: **Method and System for Configuring and Scheduling Audits of a Computer Network**	Confirmation No.: **2476**

APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

In support of the notice of appeal mailed on December 8, 2006 in the above referenced application, Appellants hereby submit this brief under 37 C.F.R. § 1.191 to appeal the Examiner's rejection of this application as reported in the Official Action mailed on October 18, 2006.

I hereby certify that this correspondence is being facsimile transmitted to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450, Facsimile No. (571) 273-8300, on December 8, 2006.

Kerry L. Broome

Kerry L. Broome, Reg. No. 54,004

Table of Contents

Real Party in Interest

The real party in interest is IBM Internet Security Services, formerly operating as Internet Security Systems, Inc., the assignee of record.

Related Appeals and Interferences

None.

Status of Claims

Claims 1-5, 7-9, 11-13, 15-17, 19-27, 29-36, and 38-45 stand finally rejected and are on appeal. Claim 10 is objected to. Claims 6, 14, 18, 28, and 37 are canceled. Appeal is taken from the rejection of all pending claims.

Status of Amendments

No additional amendments have been filed subsequent to the final rejection mailed on October 18, 2006.

Summary of Claimed Subject Matter

In general, the invention disclosed by the present application defines a new system and process that facilitates the configuration and scheduling of security audits on machines in a distributed computer network. More specifically, a security auditing system collects initial information about the identity and importance of elements in a computing network. Using this initial information, automatic selection and scheduling of security audit scans are completed on the network elements. A user can provide parameters, if so desired, as to when to schedule audit scans and what types of audit scans to run. Taking the information collected from the audit scan, the security auditing system can compute a security score for a network element based on its vulnerability and importance. The security score can be presented to the user in a manageable format to facilitate interpretation and response. The user may use the security score as a basis for adjusting the scheduling and configuration of future audit scans.

Independent Claim 1 is directed to a computer-implemented method for configuring and scheduling a security audit of a computer network. The computer implemented method comprises the following steps, along with the associated portions of the specification that support these steps: (1) conducting a discovery scan to identify an element of the computer network and determine the element's functions and assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network (page 7, lines 10-15 and page 14, lines 1-14); (2) configuring an audit scan to perform on the element, wherein the audit scan is a broader scan than the discovery scan (page 7, lines 16-26); (3) scheduling a time to perform the audit scan on the element (page 12, lines 3-22); (4) running the audit scan of the element at the scheduled time (page 12, lines 23-30); (5) calculating a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element (page 15, line 14 to page 16, line 4); and (6) scheduling another time to repeat the audit scan on the element, the scheduling based on the results of the audit scan and the security score (page 11, line 28 to page 13, line 20).

Independent Claim 13 is directed to a computer-implemented method for configuring and scheduling a security audit of a computer network. The computer implemented method comprises the following steps, along with the associated portions of the specification that support these steps: (1) conducting a discovery scan to identify an element of the computer network and

assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network (page 7, lines 10-15 and page 14, lines 1-14); (2) configuring an audit scan to perform on the element (page 7, lines 16-26); (3) scheduling a time to perform the audit scan on the element (page 12, lines 3-22); (4) running the audit scan at the scheduled time on the element (page 12, lines 23-30); and (5) calculating a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element (page 15, line 14 to page 16, line 4).

Independent Claim 22 is directed to a method for assessing the security of a network. The method comprises the following steps, along with the associated portions of the specification that support these steps: (1) receiving an initial scan identifying a network element and the function of the network element and assigning an asset value for the network element, wherein the asset value indicates the relative importance of the network element in the network (page 7, lines 10-15 and page 14, lines 1-14); (2) selecting an audit scan to perform on the network element, the selection based on the initial scan, wherein the audit scan is broader than the initial scan (page 7, lines 16-26); (3) scheduling the audit scan to perform on the network element (page 12, lines 3-22); (4) performing the audit scan on the network element at the scheduled time (page 12, lines 23-30); (5) receiving data from the selected audit scan of the network element (page 13, lines 1-20); and (6) computing a security score for the network element from the selected audit scan by summing one or more vulnerabilities associated with the network element (page 15, line 14 to page 16, line 4).

Independent Claim 30 is directed to a method for assessing the security of a network. The method comprises the following steps, along with the associated portions of the specification that support these steps: (1) receiving an initial scan identifying a network element and assigning an asset value for the network element, wherein the asset value indicates the relative importance of the network element in the network (page 7, lines 10-15 and page 14, lines 1-14); (2) selecting an audit scan to perform on the network element, said selection based on the initial scan (page 7, lines 16-26); (3) performing the selected audit scan on the network (page 12, lines 23-30); (4) receiving data from the selected audit scan of the network element (page 13, lines 1-20); and (5) computing a security score for the network element from the selected audit scan by summing one or more vulnerabilities associated with the network element (page 15, line 14 to page 16, line 4).

Independent Claim 39 is directed to a system for configuring and scheduling a security audit of a computer network. The system comprises the following elements, along with the associated portions of the specification that support these elements: (1) the computer network (Figure 1 (110); page 7, line 12 to page 8, line 26); (2) a security audit system (Figure 1 (115)) operable for conducting a discovery scan to identify an element of the computer network and assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network (page 7, lines 10-15; page 14, lines 1-14), configuring and scheduling an audit scan of the element (page 7, lines 16-26; page 12, lines 3-22), and computing a security score for the network element from the selected audit scan by summing one or more vulnerabilities associated with the network element (page 15, line 14 to page 16, line 4); and (3) a console (Figure 1 (105)) operable for receiving information from the security audit system and transmitting information to the security audit system about the discovery scan and the audit scan (page 7, line 12 to page 8, line 16).

Grounds of Rejection to be Reviewed on Appeal

The following issue is presented on appeal:

(1) Whether Claims 1-5, 7-9, 11-13, 15-17, 19-27, 29-36, and 38-45 are obvious under 35 U.S.C. § 103(a) over U.S. Patent No. 6,530,024 (Proctor); U.S. Patent No. 6,301,668 (Gleichauf), U.S. Patent No. 6,574,737 (Kingsford), U.S. Patent No. 6,889,168 (Hartley), U.S. Patent No. 6,467,002 (Yang), U.S. Patent No. 6,220,768 (Barroux), and/or U.S. Patent No. 5,715,395 (Brabson).

Argument

Rejection of claims as obvious over 35 U.S.C. § 103(a)

The Legal Standard for 35 U.S.C. § 103(a)

The U.S. patent and Trademark Office has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Warner et al.*, 379 F.2d 1011, 154 U.S.P.Q. 173, 177 (C.C.P.A. 1967), *In re Fine*, 837 F.2d 1071, 1074, 5 U.S.P.Q.2d 1596, 1598-99 (Fed. Cir. 1988). To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicants' disclosure. *In re Vaeck, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991).* The references cited by the Examiner do not meet all three criteria.

The prior art must provide one of ordinary skill in the art with the motivation to make the proposed modification needed to arrive at the claimed invention. *In re Geiger*, 815 F.2d 686, 2 U.S.P.Q.2d 1276 (Fed. Cir. 1987); *in re Lalu and Foulletier*, 747 F.2d 703, 705, 223 U.S.P.Q. 1257, 1258 (Fed. Cir. 1984). Claims for an invention are not *prima facie* obvious if the primary references do not suggest all elements of the claimed invention and the prior art does not suggest the modifications that would bring the primary references into conformity with the application claims. *In re Fritch*, 23 U.S.P.Q.2d, 1780 (Fed. Cir. 1992). *In re Laskowski*, 871 F.2d 115 (Fed. Cir. 1989). This is not possible when the claimed invention achieves more than what any or all of the prior art reference allegedly suggest, expressly or by reasonable implication.

The Court of Appeals for the Federal Circuit warned that "the best defense against the subtle but powerful attraction of a hindsight-based obviousness analysis is rigorous application of the requirement for showing of the describing or motivation to combine prior art references." *In re Dembiczak*, 175 F.3d 994 at 999 (Fed. Cir. 1999). The Examiner has not provided such a showing.

It is clear that to establish a rejection under 35 U.S.C. § 103 the cited references must (1) recite each element of the claims, (2) provide one of skill in the art with the motivation to combine the cited reference as applications have done and (3) provide one of ordinary skill in the art with a reasonable expectation of success. The references cited by the Examiner clearly do not meet all three criteria and the current rejection of the claims-in-issue lack proper support.

Analysis

The Proctor, Gleichauf, Kingsford, Hartley, Yang, Barroux, and/or Brabson references disclosed by Examiner for the rejection of independent Claims 1, 13, 22, 30, and 39 under 35 U.S.C. § 103(a) fail to disclose at least two recitations that are present in each of the independent claims. Specifically, as rejected by the Examiner in the Final Office Action mailed on 10/18/06, (1) the Yang reference fails to disclose or suggest the claimed feature of "assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network" and (2) the Kingsford reference fails to disclose or suggest the claimed feature of "calculating a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element."

As noted, independent Claims 1, 13, 22, 30, and 39 are subject to the same ground of rejection as allegedly being obvious under 35 U.S.C. § 103(a) in view of the cited references. Therefore, Applicants will group all of the independent claims on appeal and argue these particular claim recitations with respect to independent Claim 1 only.

Independent Claims 1, 13, 22, 30, and 39

Yang does not disclose or suggest the claimed feature of "assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network"

On pages 42-43 of the Final Office Action mailed on 10/18/06, the Examiner directs the Applicants' attention to Column 4, lines 40-42 of Yang, which discloses that "arbiter 101 determines the sequential order in which the requesting devices is granted access to shared resource 199A based on a priority arbitration scheme." Furthermore, the Examiner points to Column 2, lines 44-46 of Yang, which states that "[s]pecifically, in one embodiment, the present

invention assigns an initial priority order to the plurality of devices such that those devices have priorities that are distinct."

In general, Yang discloses a method and system for priority arbitration in a computer environment having a shared resource capable of servicing a plurality of devices. Yang can assign an initial order to the plurality of devices such that those devices have priorities which are distinct. Next, the system can identify those of the plurality of devices which have issued service requests to the shared resource in a first clock cycle as requesting devices. Provided that there are more than one requesting device in the first clock cycle, the system can select one of the requesting devices to be serviced by the shared resource in a second clock cycle following the first clock cycle, where the selected device has the highest of the priorities among the requesting devices based on the initial priority order. The system can also reassign the priorities among the plurality of devices such that the selected device is assigned the lowest one of the priorities. See Col. 2, line 33 to Col. 3, line 4.

Furthermore, Yang merely discloses a system that assigns a priority to network devices so that "each device is assured of the opportunity to gain access to the shared resource with substantially equal likelihood." See Col. 6, lines 57-59. The assignment of the initial priority order among devices is performed upon a power on reset or other disruptive events which necessitate a re-initialization of the priority order. See Col. 5, lines 64-67. Furthermore, after a network device gains access to the shared resource, the system of Yang can reassign the priority values to allow another device access to the shared resource. See Col. 6, lines 48-65.

The "priority arbitration scheme" of Yang is different from the "asset value" as recited in amended independent Claim 1. The "priority arbitration scheme" of Yang does not indicate the relative importance of the element in the network environment. Instead, the system of Yang randomly assigns a value to each network device to promote a fair system for granting access to the shared resource to prevent conflicts that may arise as multiple devices attempt to access the shared resource. Therefore, the value of each network device in Yang has nothing to do with its relative importance on the network, but is merely a random number that only indicates the device's order in accessing the shared resource. In fact, based on the system of Yang, all of the devices in the Yang network will eventually be assigned the highest priority value to access the shared resource. This priority assignment in Yang is arbitrary and not based on the relative

importance of the network device. Applicants submit that the invention of independent Claims 1, 13, 22, 30, and 39 is not obvious over the references of record.

Kingsford does not disclose or suggest the claimed feature of "calculating a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element"

On page 43 of the Final Office Action mailed on 10/18/06, the Examiner directs the Applicants' attention to Column 19, lines 41-46 of Kingsford, which discloses that "In the preferred embodiment, vulnerabilities are assigned a risk value on a scale of 1-100, with 1-33 being low risk, 34-66 being medium risk, and 67-100 being high risk. Each system's risk and/or a collective risk profile for the penetration test can be displayed to the user on the user interface."

The Kingsford reference describes a method and system that can perform a penetration test to discover vulnerabilities in a network by using scan modules. As part of the system of Kingsford, data records are created by modules that include a "vulnerability" field. As cited by the Examiner, the vulnerability fields of Kingsford are assigned a risk value on a scale of 1-100, with 1-33 being low risk, 34-66 being medium risk, and 67-100 being high risk. *See* Col. 19, lines 37-43.

The assignment of a risk value in Kingsford is not the same as calculating a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element as recited in independent Claim 1. The system of Kingsford merely discloses assigning a risk value based on a three-tiered range and then displaying that value to the user on a user interface or through a report. Kingsford lacks the disclosure or suggestion of summing the values of different vulnerabilities to calculate a security score as required by independent Claim 1. Applicants submit that independent Claims 1, 13, 22, 30, and 39 are not obvious over the references of record.

The remarks presented above with respect to independent Claim 1 are equally applicable to independent Claims 13, 22, 30, and 39. In summary, Applicants respectfully request that the Examiner withdraw the pending rejection of independent Claims 1, 13, 22, 30, and 39.

Dependent Claims 2-5, 7-9, 11-12, 15-17, 19-21, 23-27, 29, 31-36, 38, and 40-45

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited prior art references. The Applicants also respectfully submit that the recitations of these dependent claims are of patentable significance.

In view of the foregoing, the Applicants respectfully request that the Examiner withdraw the pending rejections of dependent Claims 2-5, 7-12, 15-17, 19-21, 23-27, 29, 31-36, 38, and 40-45.

Conclusion

In view of the arguments presented herein, Applicants respectfully request that the final rejection in this matter be vacated, and that this application be returned to the examiner with instructions to enter a notice of allowance.

Respectfully submitted,

Kerry L. Broome

Kerry L. Broome
Reg. No. 54,004

KING & SPALDING LLP
1180 Peachtree Street
34th Floor
Atlanta, GA 30309
(404) 572-4600 (Telephone)
(404) 572-5134 (Facsimile)

APPENDIX 1

CLAIMS APPENDIX

1. (Previously Presented) A computer-implemented method for configuring and scheduling a security audit of a computer network comprising the steps of:

conducting a discovery scan to identify an element of the computer network and determine the element's functions and assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network;

configuring an audit scan to perform on the element, wherein the audit scan is a broader scan than the discovery scan;

scheduling a time to perform the audit scan on the element;

running the audit scan of the element at the scheduled time;

calculating a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element; and

scheduling another time to repeat the audit scan on the element, the scheduling based on the results of the audit scan and the security score.

2. (Original) The method of Claim 1, further comprising the step of configuring a subsequent audit scan of the element that is different from the audit scan.

3. (Original) The method of Claim 1, further comprising the step of receiving a blackout time during which no audit scan can be scheduled.

4. (Original) The method of Claim 1, wherein the step of conducting a discovery scan further comprises identifying the function of the element.

5. (Previously Presented) The method of Claim 1, wherein the step of conducting a discovery scan further comprises identifying the one or more vulnerabilities associated with the element.

6. (Canceled)

7. (Original) The method of Claim 6, wherein the asset value is modified based on the audit scan.

8. (Original) The method of Claim 1, further comprising the step of receiving a manually selected asset value for the element.

9. (Original) The method of Claim 1, wherein the step of configuring an audit scan comprises selecting a type of audit scan based on the discovery scan.

10. (Original) The method of Claim 1, wherein the step of configuring an audit scan comprises:

retrieving an asset value based on the discovery scan;

retrieving a scan frequency associated with the asset value, wherein the scan frequency indicates how often the scan is performed; and

assigning a role based on the discovery scan, wherein the role indicates the function of the element; and

assigning a policy based on the discovery scan, wherein the policy indicates the type of audit scan.

11. (Original) The method of Claim 1, wherein the step of configuring an audit scan comprises manually selecting the type of audit scan.

12. (Original) A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 1.

13. (Previously Presented) A computer-implemented method for configuring and scheduling a security audit of a computer network comprising the steps of:

conducting a discovery scan to identify an element of the computer network and assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network;

configuring an audit scan to perform on the element;

scheduling a time to perform the audit scan on the element;

running the audit scan at the scheduled time on the element; and

calculating a security score for the element based on the audit scan by summing one or more vulnerabilities associated with the element.

14. (Canceled)

15. (Original) The method of Claim 13, further comprising the step of scheduling another time to perform the audit scan on the element.

16. (Original) The method of Claim 13, further comprising the step of receiving a blackout time during which no audit scan can be scheduled.

17. (Previously Presented) The method of Claim 13, wherein the step of conducting a discovery scan further comprises identifying at least one of the functions or the one or more vulnerabilities associated with the element.

18. (Canceled)

19. (Original) The method of Claim 13, wherein the step of configuring an audit scan comprises:

retrieving an asset value based on the discovery scan;

retrieving a scan frequency associated with the asset value; and

assigning a role and a policy based on the discovery scan.

20. (Original) The method of Claim 13, wherein the step of configuring an audit scan comprises manually selecting the type of audit scan.

21. (Previously Presented) A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 13.

22. (Previously Presented) A method for assessing the security of a network comprising the steps of:

receiving an initial scan identifying a network element and the function of the network element and assigning an asset value for the network element, wherein the asset value indicates the relative importance of the network element in the network;

selecting an audit scan to perform on the network element, the selection based on the initial scan, wherein the audit scan is broader than the initial scan;

scheduling the audit scan to perform on the network element;

performing the audit scan on the network element at the scheduled time;

receiving data from the selected audit scan of the network element; and

computing a security score for the network element from the selected audit scan by summing one or more vulnerabilities associated with the network element.

23. (Original) The method of Claim 22, further comprising modifying the selected audit scan; said modification based on the data received from the selected audit scan.

24. (Previously Presented) The method of Claim 22, wherein the step of receiving an initial scan comprises:

identifying an operating system for the network element;

identifying a service for the network element, the service indicating the element's function; and

identifying at least one vulnerability associated with the network element.

25. (Original) The method of Claim 22, wherein the step of selecting an audit scan is based on the initial scan.

26. (Original) The method of Claim 22, wherein the step of selecting an audit scan is based on a manual input.

27. (Original) The method of Claim 22, wherein the step of scheduling the audit scan comprises checking a blackout schedule.

28. (Canceled)

29. (Original) A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 22.

30. (Previously Presented) A method for assessing the security of a network comprising the steps of:

receiving an initial scan identifying a network element and assigning an asset value for the network element, wherein the asset value indicates the relative importance of the network element in the network;

selecting an audit scan to perform on the network element, said selection based on the initial scan;

performing the selected audit scan on the network;

receiving data from the selected audit scan of the network element; and

computing a security score for the network element from the selected audit scan by summing one or more vulnerabilities associated with the network element.

31. (Original) The method of Claim 30, further comprising the step of scheduling the selected audit scan, said scheduling based on the initial scan.

32. (Original) The method of Claim 30, further comprising modifying the selected audit scan, said modification based on the data received from the selected audit scan.

33. (Previously Presented) The method of Claim 30, wherein the step of receiving an initial scan comprises:

identifying an operating system and a service for the network element; and

identifying at least one vulnerability associated with the network element.

34. (Original) The method of Claim 30, wherein the step of selecting an audit scan is based on the initial scan.

35. (Original) The method of Claim 30, wherein the step of selecting an audit scan is based on a manual input.

36. (Original) The method of Claim 30, wherein the step of scheduling the audit scan comprises checking a blackout schedule.

37. (Canceled)

38. (Original) A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 30.

39. (Previously Presented) A system for configuring and scheduling a security audit of a computer network comprising:

the computer network;

a security audit system operable for conducting a discovery scan to identify an element of the computer network and assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network, configuring and scheduling an audit scan of the element, and computing a security score for the network element from the selected audit scan by summing one or more vulnerabilities associated with the network element; and

a console operable for receiving information from the security audit system and transmitting information to the security audit system about the discovery scan and the audit scan.

40. (Previously Presented) The system of Claim 39, wherein the security audit system is further operable for conducting a discovery scan to:

identify a function for the element; and

identify at least one vulnerability for the element.

41. (Original) The system of Claim 39, wherein the security audit system checks a blackout schedule before scheduling an audit scan.

42. (Previously Presented) The system of Claim 39, wherein the security audit system further comprises a system scanning engine operable for detecting particular one of the vulnerabilities on the network element.

43. (Original) The system of Claim 39, wherein the security audit system further comprises an Internet scanning engine operable for performing a discovery scan on the network.

44. (Previously Presented) The system of Claim 39, wherein the security audit system further comprises a database scanning engine operable for detecting vulnerabilities associated with database elements within the network.

45. (Original) The system of Claim 39, wherein the security audit system further comprises an active scan engine operable for selecting, coordinating, and scheduling various discovery and audit scans to be performed on the computer network.

APPENDIX 2

EVIDENCE APPENDIX

None.

APPENDIX 3

RELATED PROCEEDINGS APPENDIX

None.